(19) Europäisches Patentamt
European Patent Office
Office ur pé n des brevets

(11) EP 0 811 955 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
10.12.1997 Bulletin 1997/50

(51) Int. Cl.[6]: **G07B 17/04**

(21) Application number: **97109204.4**

(22) Date of filing: **06.06.1997**

(84) Designated Contracting States:
AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE

(30) Priority: **06.06.1996 US 660027**

(71) Applicant: **PITNEY BOWES INC.**
Stamford Connecticut 06926-0700 (US)

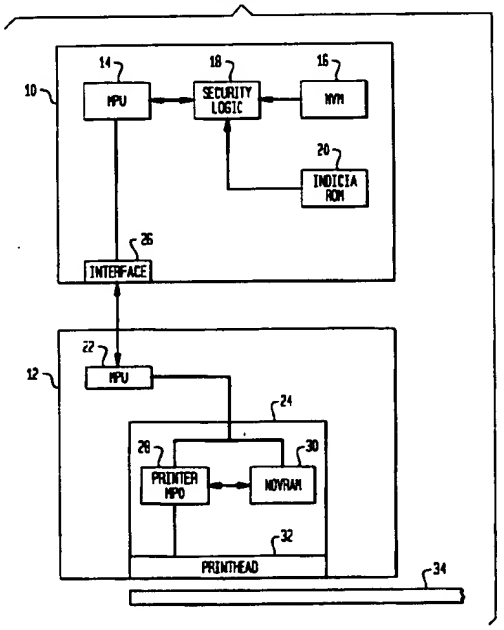
(72) Inventors:
- **Cordery, Robert A.**
  Milford, Connecticut 06811 (US)
- **D'Andrea, Thomas A.**
  Middlebury, Connecticut 06762 (US)
- **Naclerio, Edward J.**
  Madison, Connecticut 06443 (US)
- **Parkos, Maria P.**
  Milford, Connecticut 06460 (US)
- **Steinmetz, John H.**
  Bridgeport, Connecticut 06606 (US)

(74) Representative:
Avery, Stephen John et al
Hoffmann Eitle,
Patent- und Rechtsanwälte,
Arabellastrasse 4
81925 München (DE)

(54) Secure apparatus and method for printing value with a value printer

(57) A system and method of printing value such as postage using a value meter (10) connectable to communicate with a host terminal (12) which includes a printer (24). The postage meter (10), sometimes referred to as a vault, includes a processor (14) and storage (16) and the host terminal includes a processor (22) and storage (30). The printer (24) is provided with a secure non-volatile random access storage (30) and a processor (28) and a key is stored in the non-volatile random access storage (30). The key is changed for every print cycle so that it is impossible to print unauthorized postage on the basis of possession of the key used to print the last postage. A change of key is effected by reading the key from the non-volatile random access storage (30) in the printer (24) and changing the key, such as by a pseudo-random number generator, to provide a second key. The second key is stored in the non-volatile random access storage (30) and then encrypted by an encryption scheme known to an authorized postage meter. The encrypted second key is transmitted to an authorized postage meter wherein it is decrypted pursuant to the decryption scheme known to the authorized postage m ter. Print data may be securely transmitted to the host (12) and printer (24) by using the decrypted second key to convert the data to be printed. This is then sent to the printer where it is deconverted using the second key to recover the data to be printed.

FIG. 1



EP 0 811 955 A2

Descripti n

This invention relates to an apparatus and method for securely printing indicia, e.g. text and variable graphics information. The invention is applicable to such an apparatus and method wherein security is provided through cryptography.

U.S. Patents Nos. 4,802,218 and 4,864,618 issued January 31, 1989 and September 5, 1989, to Christopher B. Wright et al. describe an automated transaction system, such as a postage transaction system, in which a postage account is maintained with a microprocessor card which is used in transactions with postage printing and metering terminals. The patents particularly address security and provide for a secure handshake recognition procedure to be mutually executed between the card and the terminal so that they each recognize the other as authorized to execute a transaction.

Fig. 1 of the Wright et al. patents illustrates a postage metering terminal wherein a microprocessor card 10 is inserted in a slot 11 of the automated transaction terminal 20. The card completes multiple contacts with the terminal and a trip switch indicating full insertion triggers a start signal. The start signal is sent to an operations microprocessor or terminal MPU 30. The terminal MPU 30 controls the interface with the card and the operation of the various parts of the terminal, including the printer 40 which is the value dispensing section of the terminal. A power source Vo is provided by a battery or the like to power the various parts of the terminal.

The printer 40 contains a microprocessor unit (printer MPU) 41 which controls the operation of the printhead 42. The MPU 41 executes an internal program (FIRMWARE), as does the card microprocessor, so that it cannot be tampered with from the outside. The printer MPU's internal program includes unique encryption algorithms parallel to those stored in the card's microprocessor. These are installed by the manufacturer so that the printer MPU can execute a secure handshake recognition procedure with the card's microprocessor to authorize a requested transaction. The MPU 41 is formed integrally with the printhead 42, such as by embedding in epoxy or the like, so that it cannot be physically accessed without destroying the printhead. Thus the printhead 42 of the postage metering terminal 20 can only be operated through the MPU 41, and will print a postmark only when the handshake recognition procedure and a postmark print command have been executed between the card MPU and the printer MPU 41.

The handshake operation of the Wright et al. patents operates as follows. The card MPU 60 initiates the handshake procedure upon receipt of the commence signal. Upon verifying that the requested transaction is authorized, the card MPU encrypts an object number N, which may be a randomly generated number, with a key number k1 (which may be the printer's PIN) stored in the secret zone of its memory by a first encryption algorithm E1 and sends the resultant word W1 through the handshake channel 61 of terminal MPU 30 to the printer MPU 41.

Upon receipt of the word W1, the printer MPU 41 decodes the number using the same number k1 by the inverse algorithm E1'. The number k1 may be a secret key number stored in the printer MPU's memory at the time of validation, or in an open system, it may be the PIN entered by the user on the terminal, or a combination of both. The printer MPU 41 then encrypts the decoded number with the number k1 by a second encryption algorithm E2 to send a second word W2 back to the card MPU 60.

Upon receipt of the word W2, the card MPU 60 decodes the number again using the key number k1 by the inverse of the second algorithm E2', and compares the decoded number with the number it used in the first transmission. If the numbers-match, the handshake procedure has been successfully completed, and the card and printer MPUs have recognized each other as a authorized to execute the requested transaction.

While this handshaking protocol provides some added security, in operation it always produces the same action in response to the same input signal. Further, the printhead in the Wright et al. patents does not include hardware for storing data during periods when the power is off. The printer 40 itself is not secure. An indicia printed with the printhead of the Wright et al. arrangement can be reprinted any number of times by reproducing the electrical signal used for the first legitimate print.

It is accordingly a primary object of the present invention to provide an improved postal mailing system which may be recharged with postal funds in a secure manner so that images cannot be controlled by unauthorized users.

It is also an object of the invention to provide such a postal mailing system through the use of a secure dot addressable or the like printer.

The foregoing disadvantages of the postal mailing systems of the prior art may be overcome and the aforementioned objectives may be achieved in accordance with the invention by communication with a dot addressable or the like printhead secured by an encryption arrangement. The printhead includes a secure non-volatile static random access memory (NOVRAM) in addition to a secure application specific purpose microprocessor chip. The NOVRAM is sometimes hereinafter referred to as non-volatile memory or NVM and the specific purpose microprocessor is sometimes hereinafter referred to as an ASIC or application specific integrated circuit. According to the invention a key is changed each print cycle and stored in the NOVRAM or NVM even during times when the power is off. This access key changes for each print cycle. Thus, an unauthorized user who learns the key used for the last print cycle is unable to print an image and cannot reprint an image by reproducing the electrical signals used to print the original image.

According to the invention a printer microprocessor

unit and non-volatile static random access memory are mounted in secure fashion within the printhead. During each print cycle a number R is read from the non-volatile static random access memory (NOVRAM) in the printhead. The value of R is changed using a pseudo-random number generator and the new value is stored in the NOVRAM. The number R is encrypted using the public key of a public key encryption scheme to produce a number N. The encrypted number N is sent to the user. An authorized user has the private key for the encryption scheme and calculates R. The user takes the data that is to be printed and performs an exclusive-or operation with the binary expansion of the number R. After the exclusive-or operation the converted data is sent to the printer. The printhead takes the input converted data and again applies the exclusive-or operation to reproduce the original print data and this is printed. A significant improvement in security is provided by this use of a changing key stored in non-volatile printhead memory that allows the printhead to be accessed only by authorized users.

Embodiments of the invention will now be described with reference to the drawings, in which:

Fig. 1 is a simplified block diagram of a mailing system which may be utilized with embodiments of the invention;

Fig. 2 presents in tabular form the name, description and source of symbols, keys and other protocol data referred to in the description of secure printing according to an embodiment of the invention;

Fig. 3 is a simplified flow diagram illustrating commencement of initialization of the installation according to an embodiment of the invention;

Fig. 4 is a simplified flow diagram illustrating the graphics signing at the factory;

Fig. 5 is a simplified flowchart illustrating the initialization of the printhead graphics;

Fig. 6 is a simplified flowchart illustrating the initialization of a session;

Fig. 7 shows in simplified flowchart form a request indicia procedure;

Fig. 8 is a simplified flowchart illustration of the printing of a report procedure;

Fig. 9 sets forth in tabular form an explanation of protocol used;

Fig. 10 illustrates in tabular form protocol for signing of the graphics; and

Fig. 11 illustrates in tabular form the initialization of a session according to an embodiment of the invention.

The invention is described in further detail in the context of a postage meter, however, other types of meters may be used. Such meters include parcel service meters, tax stamp meters, check writing meters, ticket imprinters, and other similar devices.

Fig. 1 shows in a simplified block diagram a form of mailing system which may be utilized with embodiments of the invention. The mailing system may comprise a postal meter 10 which is herein referred to as an electronic vault or as a vault. The vault is in communication with a host 12 in a conventional fashion. It will be understood that the vault may take many forms, including the form of a card such as described in the Wright et al. U.S. Patents Nos. 4,802,218 and 4,864,618, referenced hereinabove. The vault may also constitute a module of more substantial size coupled to the host, such as described, for example, in U.S. Patent No. 4,858,138, issued August 15, 1989, to Paul C. Talmadge and assigned to the assignee of the instant application. Th vault includes a microprocessor (MPU) 14 which is coupled through a non-volatile memory (NVM) 16 through security logic 18. An indicia read only memory (ROM) 20, in which the particular printing indicia is stored, is also coupled to the microprocessor 14 through the security logic 18.

The host 12 includes an operations microprocessor (MPU) 22 and the printhead housing 24. The operations microprocessor 22 provides intelligence to allow for communication back and forth to vault microprocessor 14 via interface 26 to initiate printing when the proper information is exchanged. A keyboard (not shown) in the host 12 may be provided to send information representing the postage amount to the operations microprocessor 22. The printhead housing 24 is manufactured as a secure housing, and includes an operation specific printer microprocessor 28, NOVRAM 30, and printing mechanism or printhead 32 for printing indicia on a mail piece or the like 34. In a preferred embodiment the printing mechanism, NOVRAM and microprocessor constitute an integral unit.

A printhead number (Nph) is stored in the printhead NOVRAM 30 to impart a unique character to the specific printhead. Also stored in the NOVRAM 30 is a printhead seed R which is used by the printhead cryptographic pseudo-random number generator to generate nonces. The NOVRAM 30 also has stored therein in encrypted form the printhead key Kph which is the key used by the printhead and vault to generate the session key. The printhead key Kph is stored in the NOVRAM encrypted with the printhead security key Ka. The graphics key Kg, which is the key used by the manufacturer and printhead to secure graphics and other printhead data, is also stored in the NOVRAM encrypted with Ka. The printhead security key Ka is itself stored in the printhead ASIC. The printhead master key Kphm is stored securely in the vault. This key is used by the vault to cal-

culate the printhead key from the printhead number. The vault security key Kv is stored in the vault ASIC. This key is used by the vault ASIC to encrypt secret information stored in NVM.

For convenience of reference the foregoing symbols are presented in tabular form in Fig. 2 showing the symbol name, description and source. The abbreviated form NVM is used for NOVRAM in the Fig. 2 table. Fig. 2 also identifies the session nonce Ns, vault nonce Nv, indicia nonce Ni and session key Ks. The session nonce Ns is generated by the printhead with the printhead seed R and the printhead key Kph to assure session freshness. The vault nonce Nv is a pseudo-random number generated in the vault to assure that the printhead is present at the beginning of a session. The indicia nonce Ni is a nonce generated with R and Kph by the printhead to ensure indicia freshness. The session key Ks is the key used by the printhead and vault to communicate during one session. The session key is generated from Ns and Kph. The printhead key is good for initializing sessions with the vault. The graphics key is good for authenticating graphics from the vendor.

In an alternate embodiment, the number R is read from the NOVRAM 30 and the value of R is changed using a pseudo-random number generator and the new value is stored in NOVRAM 30. The number R is encrypted using the public key K_public of a public key encryption scheme to produce a number N=f(R,K_public). The encrypted number N is sent to the user. An authorized user has the private key K_private for this encryption scheme. The user calculates R=f-1(N,K_private). The user takes the data that is to be printed and performs an exclusive-or operation with the binary expansion of the number R. R may typically contain 1,000 bits and the print data may require multiple copies of R to convert all of the data. After the exclusive-or operation the converted data is sent to the printer.

The following is an exemplary illustration of the process:

Assume that R is only eight digits long and that 24 bits of print data are required.

Assume that the original value of R is 01101111. The printhead microprocessor applies a random number generator and stores a new value 10011101.

The printhead microprocessor encrypts this number to obtain f(R,K_public)=00011101 and sends this number to the user.

The user calculates f-1(000111101, K_private)= 10011101.

To print the data the user performs an exclusive-or operation with R and sends the data to the printhead:

10011101,10011101,10011101
P repeated enough times to cover the data.
00000111,01110001,11110000
Print data.
10011010,11101100,01101101
Converted print data.

The printhead takes the input converted data and again applies the exclusive-or operation to reproduce the original print data:

10011011,11101100,01101101
Converted print data.
10011101,10011101,10011101
R repeated enough times to cover the data.
00000111,01110001,11110000
Data used to print is the same as the original print data.

It will be apparent to those skilled in the art that other schemes may be used to encrypt the communication and to convert the print data. The important feature is that the system uses a changing key stored in non-volatile secure printhead memory that allows the printhead to be accessed only by authorized users.

A typical initialization of the system for a printing operation is now described in conjunction with a series of flow diagrams commencing with the simplified flow diagram of Fig. 3. Referring to that figure the printhead security key Ka is installed in the printhead ASIC at 36. This universal key secures data external to the printhead ASIC. The vault security key Kv is installed in the vault ASIC at 38. This universal key secures data external to the vault ASIC and requires an update to the ASIC. At 40 the printhead number Nph is installed in NVM in the printhead. Each printhead should have a unique number to initialize it. This is required in order that the software random number generators on different printheads produce different numbers.

The encrypted printhead key {Kph}Ka is installed in NVM at 42. The printhead key is derived by the vault from the printhead number using the printhead master key. The printhead needs the printhead key encrypted with the printhead security key. This separation ensures that an attacker who opens and deciphers everything in one printhead will not possess sufficient information to use a second or other printheads.

At 44 the encrypted graphic key {Kg}Ka is installed in NVM. This is a universal key that secures the graphics. It is not built in the ASIC in order to provide the option of changing the key in the future.

At 46 the printhead master key Kphm is installed in the vault. This is a universal key used by the vault to communicate with printheads. The vault believes that the printhead master key is good for deriving the printhead key from the printhead number.

The graphics signing at the factory is illustrated in the flowchart of Fig. 4. Referring to that figure graphics are assigned at the factory with the graphics key at 48. The vendor should be able to rely on the graphics key as a good key for authenticating graphics to the printhead and have reasonable assurance that the printhead is protected from producing counterfeit images by the graphics key. Two practical methods are available for signing graphics. In one method a message authentication code is generated by chaining DES encryptions. In an alternate method a CRC is generated with a secret

polynomial and the polynomial is encrypted. Chaining DES encryptions is commonly used in financial applications to assure message integrity. A label can be attached to the graphics indicating the type of image and the label and graphics signed together. The indicia graphics are assigned at 50. The indicia graphics include information about the location of fields so that attackers cannot permute characters in the indicia. The slogan graphics are assigned at 52 and the font graphics assigned at 54. The font graphics label includes the ASCII character represented. The permit graphics are assigned at 56.

The initialization of the printhead graphics is illustrated in Fig. 5. Referring to Fig. 5 the printhead graphics are initialized with the graphics key at 58. The graphics key is decrypted with the printhead security key at 60 and the indicia graphics are loaded and verified at 62. The graphics are loaded into the printhead NOVRAM. They are cryptographically verified each time they are loaded and a bit is set that indicates acceptance of the signature of the graphics. The add slogan graphics are loaded at 64 and a bit set that indicates acceptance of the signature of those graphics. The font graphics are loaded and verified at 66 and a bit set that indicates acceptance of the signature of those graphics. At 68 the permit graphics are loaded and verified and a bit set that indicates acceptance of the graphics signature.

The initialization of a session is illustrated in simplified flowchart form in Fig. 6. The printhead believes that the session key is authentic for communicating with the vault and believes that the vault "meter number" is also authentic. The vault believes that the session key is good for communicating with the printhead.

At 70 the printhead key is decrypted with the printhead security key. The printhead outputs a number and session nonce at 72. The printhead calculates the session key from the printhead key and nonce at 74 and the vault generates the printhead key from Nph with the printhead master key at 76. At 78 the vault calculates the session key from the printhead key and nonce. At 80 the vault sends the meter number, session nonce (and vault nonce) encrypted with the session key. The vault nonce authenticates the printhead to the vault. This assures the vault that the data it is sending is in fact going to a printhead. The printhead verifies the session nonce, saves the meter number and outputs the vault nonce at 82. The vault verifies the vault nonce at 84.

Fig. 7 shows in simplified flowchart form a request indicia print procedure. The printhead believes that the vault believes the "indicia number, piece count, postage." At 86 the printhead outputs the indicia nonce. The printhead seed is updated after each nonce. The vault encrypts the piece count, postage, (date), indicia nonce with the session key at 88. At 90 the printhead decrypts the piece count, postage, and indicia nonce.

The printing of a report procedure is illustrated in flowchart form in Fig. 8. The printhead believes that the vault believes the report and that the image represents the report. The verifier believes the vault articulated the report. At 92 the printhead sends the report nonce. The printhead and vault derive the session key at 94 and the vault encrypts the numerical data in the report at 96. The printhead verifies the font data in the report at 98 and indicates it needs a signed "format" for the report at 100.

The protocol is set forth in tabular form in Fig. 9. The principles in the protocol are V-vault, P-printhead, and M-manufacturer. The notation for encryption is that {M}K is the message M encrypted with the key K. The notation for signing is that [M]K is the message M signed with the key K. The printhead key is encrypted in NVM in a way that the printhead does not know the map from the printhead number to the printhead key. The steps indicated and described in Fig. 9 are performed under the security of the manufacturing process.

The protocol for the signing of the graphics is illustrated in tabular form in Fig. 10. When the printhead graphics are initialized at the customer site the required messages from 7-11 in Fig. 10 are sent to the printhead, verified and installed. The channel need not be particularly secure. An ad slogan could be used, if desired. The images should be reasonably well scrambled, in a way that the customer cannot easily reverse the scrambling.

As each graphic image is verified a bit is set to indicate that that image is accepted. This prevents attacks where bogus images are loaded and the printhead is powered down before it clears the data. The printhead is now initialized. A session is initialized as shown in tabular form in Fig. 11.

In step 12 the printhead generates a new nonce Ns for the session. The printhead calculates the session key Ks from the nonce by decrypting Kph from NVM and encrypting Ns. The vault calculates Ks by encrypting Nph with Kphm. At step 13 the vault sends Nv encrypted to provide assurance that the printhead is present. The printhead verifies the encrypted Ns to verify that the vault is valid. The indicia serial number is sent at this point to avoid having to send it for each indicia. The printhead decrypts the message and verifies Ns. At step 14 the vault verifies the printhead retrieved Nv to authenticate the printhead. The vault and printhead are now ready to print indicia and the session is now initialized. At step 15 for each indicia the printhead generates a nonce to assure that the indicia is fresh. At step 16 the vault prepares a message with the indicia information and the indicia nonce, encrypts it, and sends it to the printhead. The printhead verifies the indicia nonce is encrypted, loads the data into the imag , and prints the indicia.

It will be readily seen by one of ordinary skill in the art that the present invention fulfills all of the objects set forth above. After reading the foregoing specification, one of ordinary skill will be able to effect various changes, substitutions of equivalents and various other aspects of the invention as broadly disclosed herein. It is therefore intended that the protection granted hereon be limited only by the definition contained in the

appended claims and equivalents thereof.

Claims

1. In a value printing system comprising a value meter device (10) connectable to communicate with a host device (12) which includes a printer device (24) for printing value indicia pursuant to signals from said value meter device (10), said value meter device including a processor (14) and storage (16), and said host device (12) including a processor (22) and storage (30), a method comprising the steps of:

   providing in said printer device (24) a secure non-volatile random access storage (30) connected to a processor (28);
   storing a key in said printer device non-volatile random access storage (30);
   initiating a print cycle of said printer device (24) to print value indicia including print data transmitted by said value metering device (10) to said printing device (24) following mutual authentication of said key by said value meter device (10) and said printer device (24) and authentication of said print data by said printer device;
   printing said indicia including said print data and terminating said print cycle; and
   changing said key in said printer device non-volatile random access storage (30) before initiating another print cycle.

2. A method according to Claim 1, wherein said changing of said key and said authentication includes the steps of:

   reading said key from said non-volatile random access storage (30) in said printer device (24);
   changing said key to provide a second key;
   storing said second key in said non-volatile random access storage (30) in said printer device (24);
   encrypting said second key by an encryption protocol known to an authorized value metering device;
   sending the encrypted second key to an authorized value metering device; and
   decrypting said second key in said authorized value metering device.

3. A method according to Claim 2 including the steps of:

   using the decrypted second key to convert data to be printed;
   sending said data to be printed converted with said second key to said printer device (24);
   deconverting said converted data to be printed in said printer device (24) with said second key to recover the data to be printed; and
   printing said data.

4. A method according to Claim 2 or 3, wherein said key is changed to said second key by a pseudo-random number generator in said printer device.

5. A method according to Claim 1, 2, 3 or 4, wherein said processor (28) connected to said non-volatile random access storage (30) is provided in said printing device (24).

6. A method according to any one of the preceding claims, wherein said value printing system comprises a mailing system and said value meter device (10) comprises a postage meter and said printer device comprises a postage printer (24).

7. A printing module (24) for use in a value printing system (10, 12) for controlling the printing of value indicia wherein said system includes a value metering device (10) having a data processor (14) and storage (16), and a terminal (12) associated with said printing module (24), and means (26) for removably connecting said terminal (12) to said value metering device (10) for data communication between said value metering device and said terminal and said printing module, said printing module (24) comprising a data controlled printing mechanism (32) having securely mounted therewith a data processor (28) and a non-volatile random access storage (30) having a key stored therein.

8. A printing module according to Claim 7, wherein said data processor (28) and non-volatile random access storage (30) are integral with said printing mechanism (24).

9. A printing module according to Claim 7 or 8, wherein said data processor (28) and non-volatile storage (30) of said printing module (24) have stored therein a number generating protocol which operates on said key to produce a second key and an encryption protocol which operates on said second key to encrypt said key, said printing module (24) responding to transfer of data thereto by said terminal (12) when said terminal is connected to a metering device (10) having a second key to said encryption protocol to conduct a print cycle, said data processor (28) and non-volatile storage (30) of said printing module (24) having also stored therein a protocol which changes said second key before another print cycle can be conducted.

10. A printing module according to Claim 7, 8 or 9, wherein said printing module (24) is incapable of executing two successive print cycles in response to the input thereto of identical data to initiate said print cycles.

11. A value printing system for controlling the printing of value indicia including a value metering module (10) having a data processor (14) and storage (16), a host terminal (12) having processing and storage capability, a connecting mechanism (26) for removable connecting said value metering module (10) to said host terminal (12) for data transfer therebetween, and a printing module (24) secured to said host terminal (12) for data communication therewith, said printing module (24) having a data controlled printing mechanism (32) including integrally therewith a data processor (28) and a non-volatile random access storage (30) having stored therein a key for initiating a print cycle and a protocol for changing said key before another print cycle can be conducted.

12. A value printing system according to Claim 11, wherein said data processor (28) and non-volatile storage (30) of said printing module (24) have stored therein a number generating protocol for operating on a prime key stored in said non-volatile storage (30) to produce said changed key and an encryption protocol for operating on said changed key to encrypt said changed key, said printing module (24) being responsive to transfer of data thereto by said terminal (12) when said terminal is connected to a metering device (10) having a key to said encryption protocol to authenticate said changed key, said encryption protocol being arranged to change said changed key before yet another print cycle can be conducted.

13. A value printing system according to Claim 11 or 12, wherein said printing module (24) is incapable of executing two successive print cycles in response to the input thereto of identical data to initiate said print cycles.

14. A value printing system according to any one of Claims 11 to 13, wherein said value printing system (10, 12) comprises a mailing system and said value meter module comprises a postage meter and said printer module comprises a postage printer.

15. In a value printing system for controlling the printing of value indicia including a value metering module (10) having a data processor (14) and storage (16), a host terminal (12) having processing and storage capability, a connecting mechanism (26) for removably connecting said value metering module (10) to said host terminal (12) for data transfer therebetweeen, and a printing module (24) secured to said host terminal (14) for data communication therewith, said printing module (24) having a data controlled printing mechanism (32), a method comprising the steps of:

mounting integrally with said printing module (24) a data processor (28) and a non-volatile random access storage (30);

storing a key in said non-volatile random access storage (30);

performing a predetermined protocol on said key to obtain a different second key;

encrypting said second key;

communicating said encrypted second key to an authorized metering module;

decrypting said second key in said metering module (10);

authenticating said decryption in said metering module (10) to said printing module (24);

conducting a printing cycle by said printing module (24) wherein data transferred to said printing module from said host terminal is printed; and

performing a predetermined protocol on said key to obtain a different third key before conducting another printing cycle.

16. A method according to Claim 15, wherein said printing module (24) is incapable of conducting two print cycles in response to input thereto of identical data to initiate said print cycles.

17. A method according to Claim 15 or 16, wherein said protocol for obtaining said second key comprises pseudo-random generation of a number.

18. A method according to any one of claims 15 to 17 including the steps of:

installing a number unique to each printing module in said module at manufacture; and

using said unique number in said pseudo-random number generation protocol so that such number generation is unique to each printing module.

19. A method according to any one of claims 15 to 18 including the steps of: using said second key to encrypt data to be printed; transmitting said encrypted print data to said printing module (24); decrypting said print data in said printing module; and printing said data.

20. A method according to any one of Claims 15 to 19 including the steps of: retrieving said key from said non-volatile random access storage (30) and performing said protocol on said retrieved key to obtain said second key;

storing said second key in said non-volatile random access storage (30); and

retrieving said second key from said non-volatile random access storage (30) to encrypt said second key.

FIG. 1

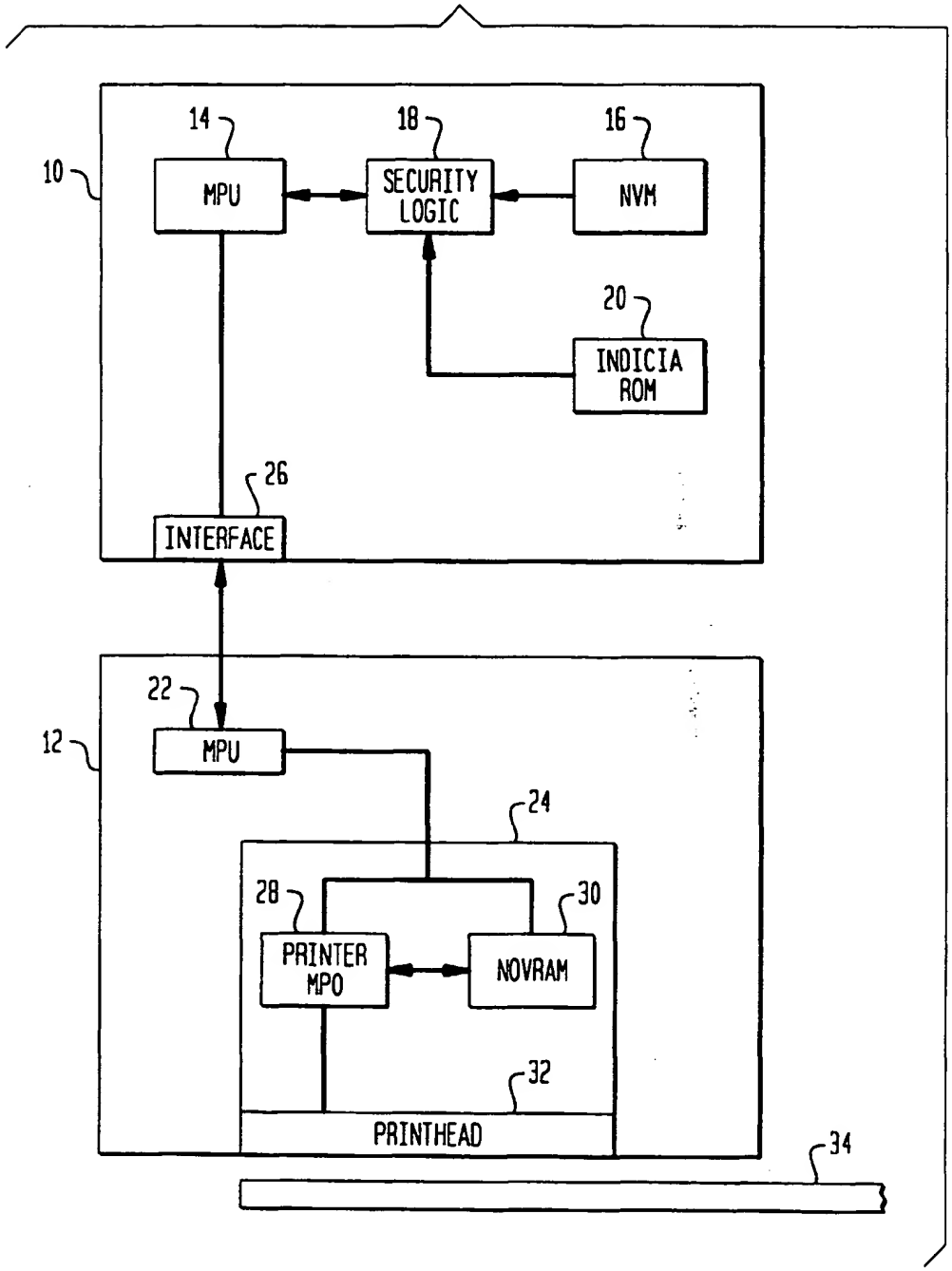

10
14
MPU
18
SECURITY LOGIC
16
NVM
20
INDICIA ROM
26
INTERFACE
12
22
MPU
24
28
PRINTER MPO
30
NOVRAM
32
PRINTHEAD
34

FIG. 2

NAME	SYMBOL	DESCRIPTION	SOURCE
SESSION NONCE	Ns	NONCE GENERATED BY PRINT HEAD TO ASSURE SESSION FRESHNESS	GENERATED WITH R AND Kph
VAULT NONCE	Nv	NONCE GENERATED BY VAULT TO ASSURE THAT PRINT HEAD IS PRESENT AT BEGINNING OF SESSION	(PSEUDO)-RANDOM NUMBER GENERATED IN VAULT
INDICIA NONCE	Ni	NONCE GENERATED BY PRINT HEAD TO ASSURE INDICIA FRESHNESS	GENERATED R AND Kph
PRINT HEAD SEED	R	SEED USED BY PRINT HEAD CRYPTOGRAPHIC PSEUDORANDOM NUMBER GENERATOR TO GENERATE NONCES	STORED IN NVM, UPDATED EACH NONCE.
PRINT HEAD NUMBER	Nph	NUMBER STORED IN PRINT HEAD NVM THAT MAKES EACH PRINT HEAD MORE OR LESS UNIQUE	STORED IN NVM, NEED NOT BE UNIQUE, OR TRACKED, BUT THERE SHOULD BE A LOT OF THEM
SESSION KEY	Ks	KEY USED BY PRINT HEAD AND VAULT TO COMMUNICATE DURING ONE SESSION	GENERATED FROM Ns AND Kph
PRINT HEAD KEY	Kph	KEY USED BY PRINT HEAD AND VAULT TO GENERATE SESSION KEY	STORED ENCRYPTED WITH Ka IN NVM
GRAPHICS KEY	Kg	KEY USED BY MANUFACTURER AND PRINT HEAD TO SECURE GRAPHICS AND OTHER PRINT HEAD DATA	STORED ENCRYPTED WITH Ka IN NVM
PRINT HEAD SECURITY KEY	Ka	KEY USED BY PRINT HEAD TO DECRYPT ENCRYPTED GRAPHICS KEY AND ENCRYPTED PRINT HEAD KEY STORED IN PRINT HEAD NVM	STORED IN PRINT HEAD ASIC
PRINT HEAD MASTER KEY	Kphm	KEY USED BY VAULT TO CALCULATE PRINT HEAD KEY FROM PRINT HEAD NUMBER	STORE SECURELY IN VAULT
VAULT SECURITY KEY	Kv	KEY USED BY VAULT ASIC TO ENCRYPT SECRET INFORMATION STORED IN NVM	STORED IN VAULT ASIC

EP 0 811 955 A2

FIG. 3

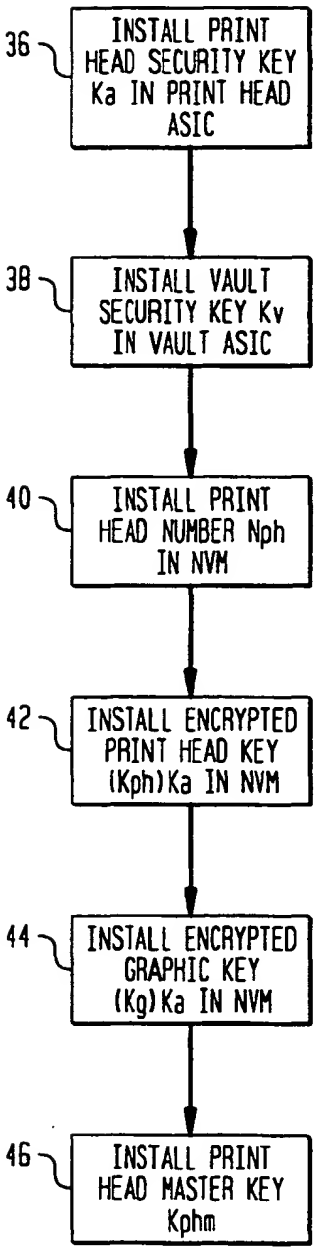

36
INSTALL PRINT HEAD SECURITY KEY Ka IN PRINT HEAD ASIC
38
INSTALL VAULT SECURITY KEY Kv IN VAULT ASIC
40
INSTALL PRINT HEAD NUMBER Nph IN NVM
42
INSTALL ENCRYPTED PRINT HEAD KEY (Kph)Ka IN NVM
44
INSTALL ENCRYPTED GRAPHIC KEY (Kg)Ka IN NVM
46
INSTALL PRINT HEAD MASTER KEY Kphm

FIG. 4

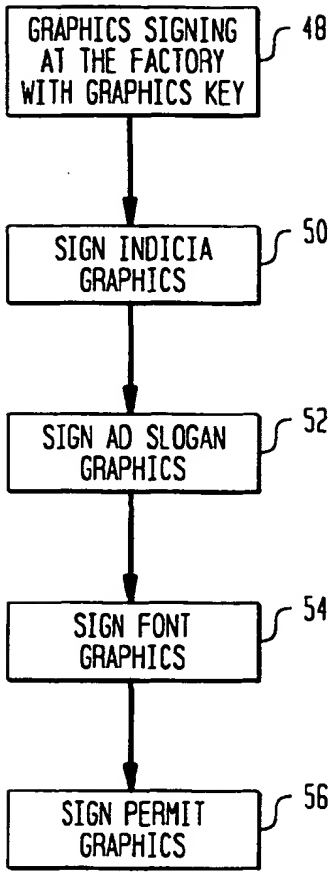

GRAPHICS SIGNING AT THE FACTORY WITH GRAPHICS KEY
48
SIGN INDICIA GRAPHICS
50
SIGN AD SLOGAN GRAPHICS
52
SIGN FONT GRAPHICS
54
SIGN PERMIT GRAPHICS
56

FIG. 5

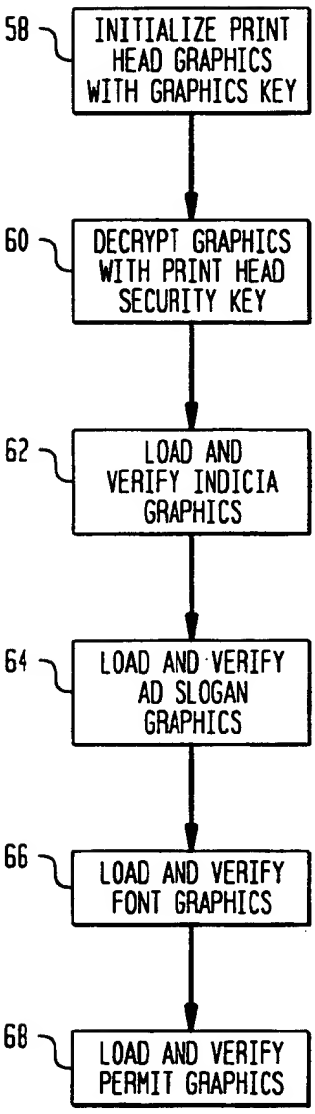

58
INITIALIZE PRINT HEAD GRAPHICS WITH GRAPHICS KEY
60
DECRYPT GRAPHICS WITH PRINT HEAD SECURITY KEY
62
LOAD AND VERIFY INDICIA GRAPHICS
64
LOAD AND VERIFY AD SLOGAN GRAPHICS
66
LOAD AND VERIFY FONT GRAPHICS
68
LOAD AND VERIFY PERMIT GRAPHICS

FIG. 6

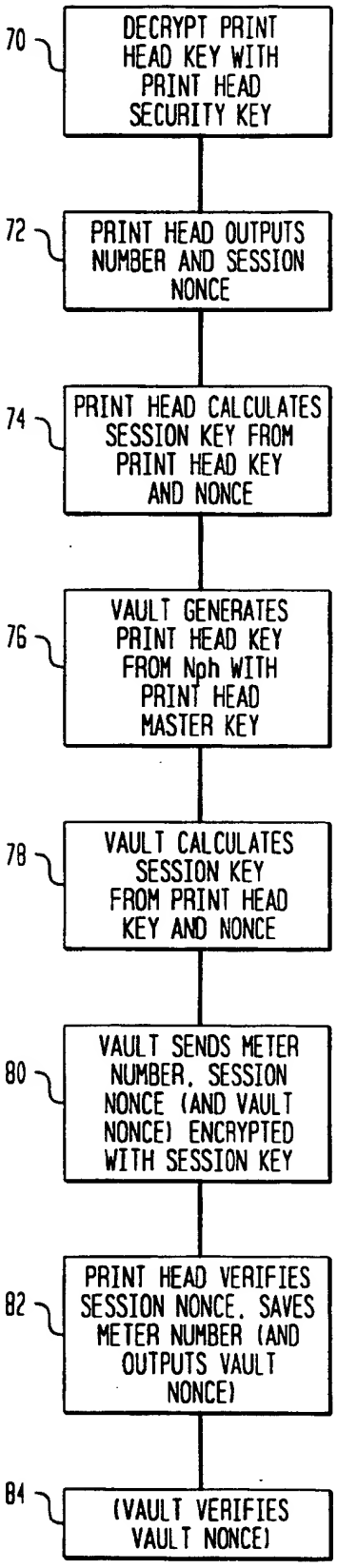

70
DECRYPT PRINT HEAD KEY WITH PRINT HEAD SECURITY KEY
72
PRINT HEAD OUTPUTS NUMBER AND SESSION NONCE
74
PRINT HEAD CALCULATES SESSION KEY FROM PRINT HEAD KEY AND NONCE
76
VAULT GENERATES PRINT HEAD KEY FROM Nph WITH PRINT HEAD MASTER KEY
78
VAULT CALCULATES SESSION KEY FROM PRINT HEAD KEY AND NONCE
80
VAULT SENDS METER NUMBER, SESSION NONCE (AND VAULT NONCE) ENCRYPTED WITH SESSION KEY
82
PRINT HEAD VERIFIES SESSION NONCE, SAVES METER NUMBER (AND OUTPUTS VAULT NONCE)
84
(VAULT VERIFIES VAULT NONCE)

FIG. 7

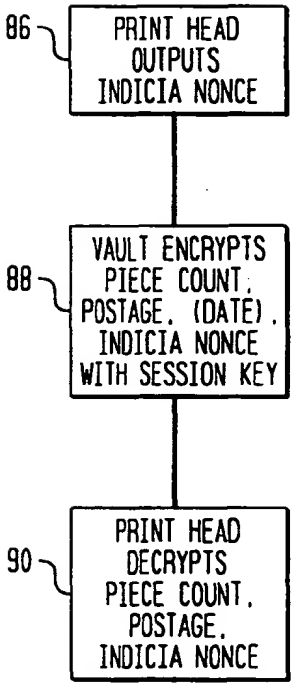

86
PRINT HEAD OUTPUTS INDICIA NONCE
88
VAULT ENCRYPTS PIECE COUNT, POSTAGE, (DATE), INDICIA NONCE WITH SESSION KEY
90
PRINT HEAD DECRYPTS PIECE COUNT, POSTAGE, INDICIA NONCE

FIG. 8

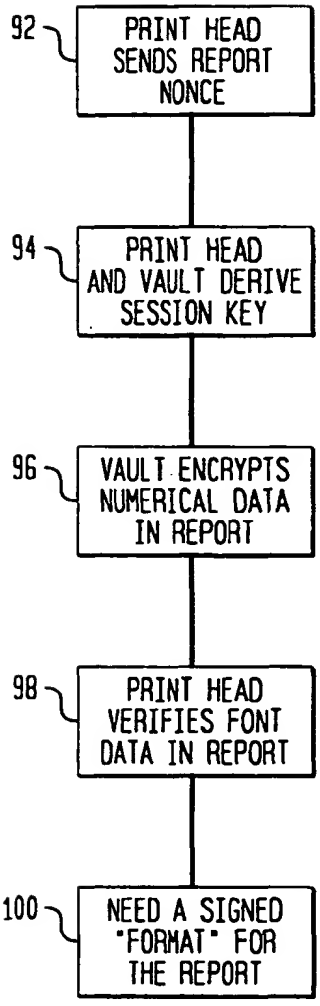

92
PRINT HEAD SENDS REPORT NONCE
94
PRINT HEAD AND VAULT DERIVE SESSION KEY
96
VAULT ENCRYPTS NUMERICAL DATA IN REPORT
98
PRINT HEAD VERIFIES FONT DATA IN REPORT
100
NEED A SIGNED "FORMAT" FOR THE REPORT

FIG. 9

THE FIRST STEPS ARE PERFORMED UNDER THE SECURITY OF THE MANUFACTURING PROCESS

1	M→P:Ka	PRINT HEAD ASIC UNIVERSAL KEY Ka IS INSTALLED IN THE PRINT HEAD ASIC. IT IS ESSENTIAL TO KEEP THIS KEY SECRET.
2	M→P:Nph	THE PRINT HEAD NUMBER IS STORED UNENCRYPTED IN NVM, AND IS DIFFERENT FOR EACH PRINT HEAD, OR AT LEAST FOR SEVERAL THOUSAND PRINT HEADS.
3	M→P:{Kph}Ka	THE PRINT HEAD KEY GENERATES THE SESSION KEYS. THE ENCRYPTED PRINT HEAD KEY IS STORED IN NVM. Kph IS A FUNCTION OF Nph: Kph = {Nph}Kphm. ONLY THE VAULT AND MANUFACTURER KNOWS Kphm.
4	M→P:{Kg}Ka	THE ENCRYPTED GRAPHICS KEY IS STORED IN NVM. THIS IS PROBABLY A UNIVERSAL KEY, BUT STORING IT ENCRYPTED IN NVM GIVES US THE FLEXIBILITY TO HAVE IT DEPEND ON POSTAL SERVICE, OR PRINT HEAD, OR MAILING MACHINE.
5	M→V:Kv	A UNIVERSAL VAULT ASIC PROTECTION KEY IS STORED IN THE THE VAULT ASIC. IT IS ESSENTIAL TO KEEP THIS KEY SECRET.
6	M→V: {Kphm}Kv	THE PRINT HEAD MASTER KEY Kphm IS ANOTHER KEY THAT IS PROBABLY UNIVERSAL, BUT THE FLEXIBILITY TO CHANGE IT COULD BE VALUABLE. Kphm SHOULD BE STORED ENCRYPTED IN THE VAULT NVM.

FIG. 10

7	M→P:[INDICIA GRAPHICS]Kg	THE GRAPHICS SIGNATURE COULD BE EITHER A CHAINED DES OR A CRC WITH A SECRET POLYNOMIAL, AND THE RESULT ENCRYPTED.
8	M→P:[LOCATION OF VARIABLE DATA IN THE INDICIA]Kg	THIS COULD BE PART OF THE PREVIOUS PROTOCOL STEP.
9	M→P:[FONT GRAPHICS]Kg	THE FONT GRAPHICS INCLUDES A CHARACTER IDENTIFIER IN THE LABEL.
10	M→P:[AD SLOGAN GRAPHICS]Kg	AD SLOGANS MUST BE SIGNED BY PB.
11	M→P:[PERMIT GRAPHICS]Kg	THE PERMIT HAS NO VARIABLE INFORMATION.

FIG. 11

12	P→V:Ns, Nph	THE PRINT HEAD GENERATES A NEW NONCE Ns FOR THE SESSION. THE PRINT HEAD CALCULATES THE SESSION KEY Ks FROM THE NONCE BY DECRYPTING Kph FROM NVM AND ENCRYPTING Ns. THE VAULT CALCULATES Ks BY ENCRYPTING Nph WITH Kphm.
13	V→P:{Ns, Nv, INDICIA SERIAL NUMBER}Ks	THE VAULT SENDS Nv ENCRYPTED TO PROVIDE ASSURANCE THAT THE PRINT HEAD IS PRESENT. THE PRINT HEAD VERIFIES THE ENCRYPTED Ns TO VERIFY THAT THE VAULT IS VALID. THE INDICIA SERIAL NUMBER IS SENT AT THIS POINT TO AVOID HAVING TO SEND IT FOR EACH INDICIA. THE PRINT HEAD DECRYPTS THE MESSAGE AND VERIFIES Ns.
14	P→V:Nv	THE VAULT VERIFIES THAT THE PRINT HEAD RETRIEVED Nv, TO AUTHENTICATE THE PRINT HEAD. THE VAULT AND PRINT HEAD ARE NOW READY TO PRINT INDICIA. THE SESSION IS NOW INITIALIZED.
15	P→V:Ni	FOR EACH INDICIA THE PRINT HEAD GENERATES A NONCE TO ASSURE THAT THE INDICIA IS FRESH.
16	V→P:{Ni, PIECE COUNT, TOKENS, DATE, POSTAGE}Ks	THE VAULT PREPARES A MESSAGE WITH THE INDICIA INFORMATION AND THE INDICIA NONCE, ENCRYPTS IT, AND SENDS IT TO THE PRINT HEAD. THE PRINT HEAD VERIFIES THE INDICIA NONCE IS ENCYPTED, LOADS THE DATA INTO THE IMAGE, AND PRINTS THE INDICIA.